STIC Search Report
EIC 2100

STIC Database Tracking Number: 116685

TO: Jerry B Dennison **Location: 3C21** **Art Unit : 2143** **Thursday, March 11, 2004** **Case Serial Number: 09/7715641**	**From: David Holloway** **Location: EIC 2100** **PK2-4B30** **Phone: 308-7794** **david.holloway@uspto.gov**

Search Notes

Dear Examiner Dennison,

Attached please find your search results for above-referenced case.
Please contact me if you have any questions or would like a re-focused search.

David

STIC EIC 2100
Search Request Form

116685
(62)

Today's Date: 3/11/04

What date would you like to use to limit the search?

Priority Date: Other:

Name J. Bret Dennison

AU 2143 Examiner # 80115

Room # 3C21 Phone 305-8756

Serial # 09/715641

Format for Search Results (Circle One):

PAPER DISK EMAIL

Where have you searched so far?

USP DWPI ~~EPO~~ ~~JPO~~ ~~ACM~~ IBM TDB

~~IEEE~~ INSPEC SPI Other _____

Is this a "Fast & Focused" Search Request? (Circle One) YES NO

A "Fast & Focused" Search is completed in 2-3 hours (maximum). The search must be on a very specific topic and meet certain criteria. The criteria are posted in EIC2100 and on the EIC2100 NPL Web Page at http://ptoweb/patents/stic/stic-tc2100.htm.

What is the topic, novelty, motivation, utility, or other specific details defining the desired focus of this search? Please include the concepts, synonyms, keywords, acronyms, definitions, strategies, and anything else that helps to describe the topic. Please attach a copy of the abstract, background, brief summary, pertinent claims and any citations of relevant art you have found.

STIC Searcher David Holloway Phone 308-7794

Date picked up 3-11-04 Date Completed 3-11-04

DTIC #

Untitled

J. Bret Dennison
AU: 2143
305-8756
Need by Monday

CASE: 09/715641

preventing spam by setting a limit to the number of emails a user can send out in a time frame.

(1) email or (electronic or electric or e) adj (mail or message)
(2) maximum adj (count or number or transmission) or (limit or quota)
(3) spam

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 March 2002 (07.03.2002)

PCT

(10) International Publication Number
WO 02/19069 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/GB01/03852

(22) International Filing Date: 29 August 2001 (29.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0021444.5 31 August 2000 (31.08.2000) GB

(71) Applicant *(for all designated States except US)*: **CONTENT TECHNOLOGIES LIMITED** [GB/GB]; 1310 Waterside, Arlington Business Park, Theale, Reading, Berkshire RG7 4SA (GB).

(72) Inventor; and

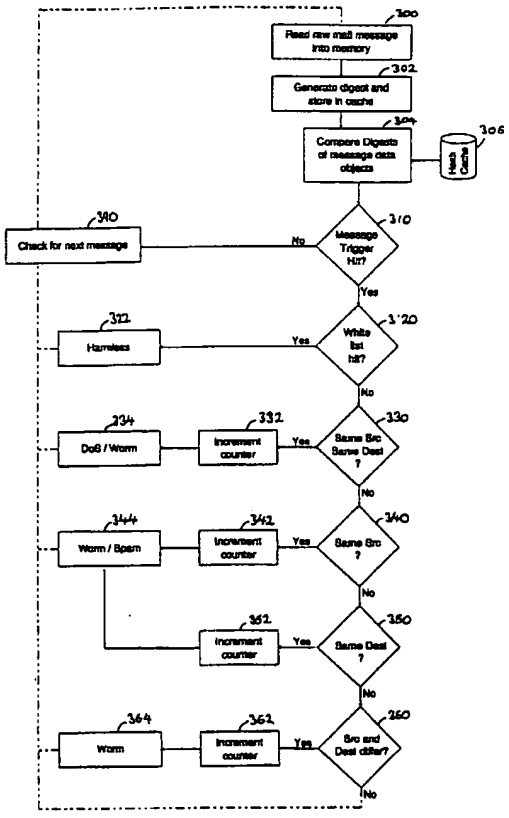
(75) Inventor/Applicant *(for US only)*: **HOCKEY, Alyn** [GB/GB]; c/o Content Technologies Limited, 1310 Waterside, Arlington Business Park, Theale, Reading, Berkshire RG7 4SA (GB).

(74) Agent: **O'CONNELL, David, Christoper**; Haseltine Lake & Co., Imperial House, 15-19 Kingsway, London WC2B 6UD (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EC, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

[Continued on next page]

(54) Title: MONITORING ELECTRONIC MAIL MESSAGE DIGESTS



(57) Abstract: A method for monitoring electronic mail messages, each mail message comprising header information and a main body, particularly for protection against virus attacks and unsolicited commercial email (UCE). The method comprises generating a summary digest of only the subject line and the message content of the main body, wherein the message content may comprise textual content and/or attached files. The generated summary digest is stored in a memory, and compared with existing summary digests stored in memory. If the number of matches exceeds a threshold value, an alert signal is raised and appropriate action initiated. A timestamp may be stored with each summary digest, together with sender/recipient details and the internet protocol (IP) address of origin, to aid detection of the originator of the message.

WO 02/19069 A2

中文

Anti-SPAM - Implementation Guideline

Version 1.0, 08-Feb-2000

Introduction

This document augments the Anti-SPAM - Code of Practice (COP) (http://www.hkispa.org.hk/antispam/cop.html) document recommended by the Hong Kong Internet Service Providers Association (HKISPA) to all its members. The purpose of this implementation guideline is to offer additional information and tips, as well as those gathered in the process of drafting the COP, for implementation of conformance to the COP. It is detached from the COP because of fast evolution of the Internet on new technologies and new applications that this implementation guideline is subject to frequent update.

Members are encouraged to contribute to this document. The latest version of this document is

available at http://www.hkispa.org.hk/antispam/guidelines.html.

Audience

This document is primarily for service providers and web site operators who or whose customers have the ability to generate electronic forms of messages, including e-mail, news, mailing list postings, etc.

Why do I need to participate in SPAM combat?

If you don't know what is SPAM you probably should learn more about it at http://spam.abuse.net/. There are a number of reasons why service providers and operators should participate in SPAM combat.

- SPAM takes up your bandwidth, mail server CPU time, and disk space that the party who send the SPAM to your server bears virtually no cost.
- Your customers do not like SPAM to fill up their inboxes. In customer service terms you should provide help to your customers to minimize the amount of SPAM they receive. That is one of the ways to keep your customers.
- If your web site or your customers generate significant amount of SPAM, your site will most probably be placed in the Realtime-Blackhole-List (http://maps.vix.com). You will soon find that many e-mail hosts start rejecting all e-mails from your servers including legitimate ones, because more and more mail servers on the Internet choose to reject all connections from servers in that blacklist.
- If your e-mail server allow open relaying, it will most probably be hijacked for SPAM transmission. You will soon find your server end up in that blacklist.
- Be a responsible corporate citizen.

Structure of this document

This document presents additional information under section headings of the COP. It should be read with the COP and act as reference and implementation notes for the COP.

Definition of SPAM

As in the COP SPAM is defined as "flooding the Internet with many copies of an electronic message that is being unsolicited, i.e. not requested by the recipient. A SPAM message will request the user to perform some kind of action e.g. go to some web site or buy some service. The message may be an e-mail but could equally be another form of electronic message such as a Usenet article."

The above definition is the minimum definition for SPAM as opined by HKISPA. Members are encouraged to consider including the above definition in their own Acceptable Use Policies. Members may further define and quantify the definition when situation or size of their operation requires. HKISPA encourage members to impose a stricter definition of SPAM according to

their own requirements.

For your reference, MCI defines SPAM as follows.

- To post ten (10) or more messages similar in content to Usenet or other newsgroups, forums, e-mail mailing lists or other similar groups or lists;
- To post to any Usenet or other newsgroup, forum, e-mail mailing list or other similar group or list articles which are off-topic according to the charter or other owner-published FAQ or description of the group or list;
- To send unsolicited e-mailings to more than twenty-five (25) e-mail users, if such unsolicited e-mailings could reasonably be expected to provoke complaints;
- To falsify user information provided to MCI or to other users of the service in connection with use of an MCI service; and
- To engage in any of the foregoing activities by using the service of another provider, but channeling such activities through an MCI account, remailer, or otherwise through an MCI service or using an MCI account as a maildrop for responses or otherwise using the services of another provider for the purpose of facilitating the foregoing activities if such use of another party's service could reasonably be expected to adversely affect an MCI service.

Terms and Conditions

Members covered by COP shall require their customers who would have the ability to produce SPAM to fall under contractual conditions such that they should not transmit SPAM or their account be terminated. Definition of SPAM should also be stated.

Members might also consider incorporating these elements into the service contract.

- More specific guidance on when the sanctions of suspension and closure of account should be imposed, e.g. should the account be suspended when customer breached the AUP for the first time?
- What will be the minimum acceptable length of suspension of service, e.g. How long after the suspension can the same e-mail account be re-activated, what is the procedure and policy, penalty, etc.
- Members might on their own consideration include in the service contract with provisions for the levying of "cleaning-up fees" on their customers who breach the AUPs. This would create a financial penalty for sending SPAM.

Technical Measures

Mail Relaying

Older versions of e-mail software allow open relaying by default. Latest versions of e-mail software have provisions for SPAM prevention, including features to deny mail relaying. If your e-mail server allows open relay, you are suggested to upgrade to a non-relay version, or remove that server from the Internet entirely. In particular,

http://www.sendmail.org/tips/relaying.html describes how to configure the most popular e-mail server Sendmail in denying open relaying, and
http://www.glenns.org/spam/sendmail/antispam.html describes how to configure other popular e-mail servers in deny open relay.

Realtime-Blackhole-List

An easy yet very useful SPAM prevention method is to use the currently free Real Time Black Hole List, currently provided by Vixie Enterprises. Latest version of the most popular e-mail server Sendmail supports use of the Real-Time-Black-Hole-List. Related information can be found at

http://maps.vix.com/
http://www.sendmail.org/antispam.html

Restriction of amount of outgoing e-mail for web e-mail and prepaid accounts

If you are offering free e-mail service or pre-paid short-term accounts, they will very likely be used for anonymous e-mail or SPAM. It is wise to limit the amount of e-mails each account can transmit per day.

Your might find the MaxRecipients limit of Sendmail version 8.10, which is still under beta testing as on 08-Feb-2000, useful.

Consult your software vendor for limitation of amount of e-mails transferred per day per account.

Deny outgoing TCP access to the Internet on port 25 (SMTP)

Professional Spammers make use of switched dialup access to get a different IP address each time and then connect to outside e-mail servers directly through a TCP connection at port number 25.

To fix this loophole, it is wise to deny TCP connection to port 25 from your dialup modems to all outside hosts. 99% of your dialup customers do not connect directly to outside hosts at port 25 but use e-mail clients (Outlook, Netscape, etc) that use the ISP's e-mail server to transmit e-mail. The remaining 1% of them either have a decent need to connect directly to outside hosts where you can cater for separately, or they are Spammers.

Denying TCP connections from your modem pool to outside hosts is best performed at your border routers. Alternatively, you can choose to direct all outgoing TCP connections to port 25 to your own e-mail server.

Incoming SPAM Filtering

It is HKISPA and OFTA's opinion that it is not economical for ISPs to filter incoming e-mails for SPAM. However if your customers request SPAM filtering service you might be interested in these information.

http://www.sendmail.org/antispam.html as starting point.

http://www.glenns.org/spam/sendmail.antispam.html for useful information on anti-SPAM provisions on various e-mail server software.

http://www.gtoal.com/spam/sendmail.html for a simple and useful score-based filter for Sendmail.

Limit NNTP Postings

It is wise to limit the use of your news servers to your own customers only. Open news servers produce the same sort of problem of open mail relays that it opens a "free entry-point" of injecting large volume of SPAM into the Internet.

Apart from limiting news posting to only your customers, modern NNTP server software have provisions for limiting the number of postings each client can post per day. Please see your NNTP software for details.

Mailing Lists

Some implementations of mailing lists software (such as Majordomo) can be configured to allow users to get all the e-mail addresses of all subscribers of specific list by a simple command. It is recommended to disable this command.

Administrative Measures

Reporting

There shall be an 'abuse' account. Mail sent to this account shall be routed to a responsible person or team who has the ability to investigate and take action on such complaints. Please be reminded that setting up an 'abuse' account alone is not enough. Proper working procedures should also be drafted to handle complaints sent to this account such that all complaints addressed to this account shall be replied to. An unresponsive 'abuse' account only tells people that this ISP is irresponsible.

Investigation and action

Service providers are responsible for investigation of all complaints forwarded to their 'abuse' account. If the complaint was verified to be legitimate and the SPAM was originated from the ISP receiving the complaint, the ISP should take action according to their own service contracts with the customer who generated the SPAM.

Situation might arise that the complainant or the party who actually generated the SPAM (or both) is not related to the ISP receiving the complaint. This will arise for a variety of reasons. For example, where the complainant complains to his or her own service provider without checking the apparent origin of the SPAM in the header or where the header information has been forged by the spammer to create a false trail that leads to the party who receives the complaint. In such cases, members receiving such complaints should make reasonable efforts to determine the true origin of the SPAM and then notify the service provider or host operator

concerned of the problem. It is recognized that the party operating the service or host from which the SPAM originated may not come under the Code, i.e. because it is outside Hong Kong or is not a member of the ISP Association. However, such a party should, as a minimum, be notified of the action of its user and the nuisance that has been caused.

Publicity

ISPs who is certified to be compliant with the COP will be published on the HKISPA web site. Members are encouraged to paste the anti-SPAM logo on their own company web site and links the logo to the anti-SPAM page of HKISPA.

Compliance

Evidence of compliance is to be submitted to Exco of HKISPA by respective ISPs showing that they have satisfied all conditions stated in the COP, which is considered a minimum standard by HKISPA.

Non-Compliance

The Executive Council of the HKISPA reserves the right to remove any party's rights to advertise compliance under the HKISPA Anti-SPAM Initiative. Such measures shall be taken if it can be shown that a party has flouted the conditions under the COP without reasonable excuse. Further action may be taken at the discretion of the Executive Council of the HKISPA.

Contact
Anti-Spam committee, HKISPA
anti-spam@hkispa.org.hk

Back

Upgrading from sendmail-8.8 to sendmail-8.9

Some new options have been added to sendmail-8.9 to provide additional control over the mailer's behaviour and take advantage of new features. Some of these options have been added to sendmail-8.8 as well.

The new options `AcceptLoad` and `DeliverLoad` control how busy the mail server is allowed to get and still accept incoming messages and deliver queued messages, respectively.

The new `MaxRecipients` option limits the maximum number of local recipients for an incoming message. The default is to refuse to deliver messages addressed to more than 128 local recipients.

The new `privacy_options` option limits what commands may be used by remote systems connecting to the mail server. This option may be used to refuse or put conditions on such things as address lookup and standards-compliant delivery status notifications.

The list of remote servers to check for spam sources has been expanded to RBL, ORBS (2), RRSS, IMRSS and DUL. See the `sendmail-config` man page or the sendmail spam info page for further information.

New Default Behaviour

Some of sendmail's default behaviour has changed to conform more closely with standard implementations.

The `phquery` mailer is deprecated and will not be directly supported in later releases of sendmail. If a mail server is expected to deliver mail for userids which may not exist on the server itself, the experimental option `local_phquery` may be used to provide this service but this feature does not support userids longer than 8 characters. People relying on the old `phquery` behaviour are strongly encouraged to publish their email address in the form `userid@uwaterloo.ca` or make mail forwarding arrangements with the system administrator of the mail server named for their preferred form of address.

Posting news articles through email is deprecated, though the functionality will continue to exist in sendmail-8.11. The default behaviour in sendmail-8.9 is to refuse to pass appropriately addressed mail messages to the campus news server. Mail to news gatewaying may be restored by setting the option `news_gateway` to yes.

The ability to relay messages from an off-campus machine after having authenticated by use of a POP or IMAP service has been changed from a system log watcher to a daemon-based method. The option to allow such authenticated relaying has been renamed from allow_pop to pop_relay and requires that the POP and IMAP servers in the `imap-4.6` or `imap-2000` package be used on the mail server.

For additional security, the default mailer for programs has been changed from the Unix shell to the more restrictive `smrsh`. This change may cause mail delivery to fail for some aliases and `.forward` files. To disable the secure shell mailer, set the option `use_secure_shell` to `no`.

The non-standard `Return-Receipt-To` header has been dropped in favour of the RFC 1891 based Delivery Status Notification in the mail transfer dialogue.